Algebraic Number Theory

Lecture 13, 21st January

K: number field
r: # real embeddings
s: # pairs of complex emb.

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau : K \to \mathbb{C}} \mathbb{C}$$
$$a \longmapsto (\tau(a)) = (a_\tau)$$

$F : z \mapsto \bar{z}$

Recall Lecture 12

$$\begin{tikzcd}
\mathcal{O}_K^\times \arrow[r, "j"] \arrow[rr, bend left, "\lambda"] \arrow[d, phantom, "\cap"] & S = N^{-1}(\pm 1) \arrow[r, "\ell"] \arrow[d, phantom, "\cap"] & H = T_r^{+}(0) \arrow[d, phantom, "\cap"] \\
K^\times \arrow[r, "j"] \arrow[d, "N_{K/L}"'] & K_{\mathbb{R}}^\times \arrow[r, "\ell"] \arrow[d, "N"'] & \left[\prod_\tau \mathbb{R}\right]^+ \cong \mathbb{R}^{r+s} \arrow[d, "Tr"] \\
\mathbb{Q}^\times \arrow[r] & \mathbb{R}^\times \arrow[r] & \mathbb{R}
\end{tikzcd}$$

$$\ell : K_{\mathbb{C}}^\times \longrightarrow \prod_\tau \mathbb{R}$$
$$(z_\tau) \longmapsto (\ell(z_\tau)) = (\log(|z_\tau|))$$

Proposition 9.1 The sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\lambda} \underset{\mathrm{im}(\Gamma)}{\underset{\parallel}{\Gamma}} \longrightarrow 0$$

is exact, i.e. $\ker \lambda = \mu(K)$.

Lemma 9.2 For a given $a \in \mathbb{Z}$, there are, up to associates, only finitely many $\alpha \in \mathcal{O}_K$ with $N_{K/\mathbb{Q}}(\alpha) = a$.

Proposition 9.3 The group $\Gamma = \lambda(\mathcal{O}_K^\times)$ is a complete lattice in the $(r+s-1)$-dimensional vectorspace H, i.e. $\Gamma \cong \mathbb{Z}^{r+s-1}$.

Theorem 9.4 (Dirichlet's unit theorem)

The unit group $\mathcal{O}_K^\times$ is given by a direct product of the cyclic group $\mu(K)$ and a free abelian group of rank $r+s-1$, i.e.

$$\mathcal{O}_K^\times \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}.$$

Remark 9.5

i) By Thm. 9.4 there exist units $\varepsilon_1, \dots, \varepsilon_t$ $(t = r+s-1)$ called the <u>fundamental units</u>, such that any unit $\varepsilon \in \mathcal{O}_K^\times$ can be written as

$$\varepsilon = \zeta \, \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$$

with $\zeta \in \mu(K)$ and $\nu_1, \dots, \nu_t \in \mathbb{Z}$.

ii) The unit group $\mathcal{O}_K^\times$ is finite iff $r+s-1=0$.

$r=1,\ s=0$: $n = [K:\mathbb{Q}] = 1 \Rightarrow K = \mathbb{Q}$.

$r=0,\ s=1$: $K = \mathbb{Q}(\sqrt{d})$ with $d<0$ square free (imag. quadratic field).

In this case $\mathcal{O}_K^\times = \{\pm 1\}$ except for

$K = \mathbb{Q}(i)$, $\mathcal{O}_K^\times = \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}$

$K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_K^\times = \left\{ \left(\frac{1+\sqrt{-3}}{2}\right)^j, j = 0, \dots, 5 \right\} \cong \mathbb{Z}/6\mathbb{Z}$

iii) For a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ ($d>0$ square free)

we have $r=2, s=0$, i.e $\mathcal{O}_K^\times$ has rank $r+s-1 = 1$ and $\mu_K = \{\pm 1\}$

$$\mathcal{O}_K^\times = \{\pm 1\} \times \mathbb{Z}.$$

Therefore there exist a unit ε such that any other unit can be written as $\pm \varepsilon^n$. ($n \in \mathbb{Z}$)

$-\varepsilon$, $\frac{1}{\varepsilon}$ and $-\frac{1}{\varepsilon}$ also satisfy this property, and among these four one usually chooses the unique one which is positive and > 1.

This is called <u>the</u> fundamental unit of K.

If $d \equiv 2, 3 \bmod 4$ we saw that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$

therefore $N_{K/\mathbb{Q}}(\underbrace{a+b\sqrt{d}}_{x}) = a^2 - b^2 d$.

If x is a unit then $a^2 - b^2 d = 1$. $(*)$ (Pell's equation)

e.g: $d=7$: In this case considering small values for b in $b^2 d$ we see that $b=3$ gives the smallest solution to $(*)$ with $a=8$.

$\Longrightarrow$ $\varepsilon = 8+3\sqrt{7}$ is the fundamental unit of $\mathbb{Q}(\sqrt{7})$.

Since $[\prod_\tau \mathbb{R}]^+ = \mathbb{R}^{r+s}$ the H can be viewed as a subspace of euclidean space.

We can ask for the volume of the fundamental mesh $\mathrm{vol}(\Gamma)$ of $\Gamma = \lambda(\mathcal{O}_K^\times) \subset H$.

Let $\varepsilon_1, \dots, \varepsilon_t$ with $t = r+s-1$ be fundamental units and set

$$H^\perp \ni \lambda^\perp = \frac{1}{\sqrt{r+s}}(1\ 1 \dots 1) \in \mathbb{R}^{r+s}.$$

$\lambda^\perp$ has length 1 and is orthogonal to H.

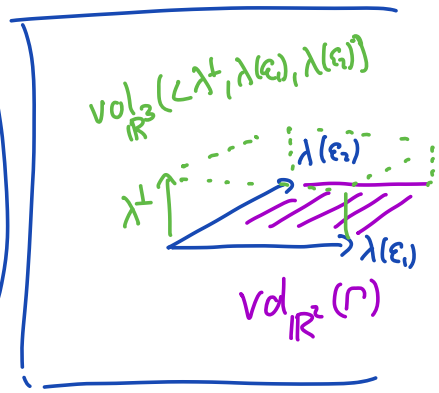
The fundamental mesh of Γ is spanned by

$$\lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)$$

and we have

$$\mathrm{vol}_{\mathbb{R}^t}(\Gamma) = \mathrm{vol}_{\mathbb{R}^{t+1}}(\langle \lambda^\perp, \lambda(\varepsilon_1), \dots, \lambda(\varepsilon_t)\rangle)$$

$$= \pm \det \begin{pmatrix} \lambda^\perp_1 & \lambda(\varepsilon_1)_1 & & \lambda(\varepsilon_t)_1 \\ \vdots & \vdots & \cdots & \vdots \\ \lambda^\perp_{t+1} & \lambda(\varepsilon_1)_{t+1} & & \lambda(\varepsilon_t)_{t+1} \end{pmatrix} \qquad (**)$$



Proposition 9.6

We have $\mathrm{vol}_{\mathbb{R}^t}(\lambda(\mathcal{O}_K^\times)) = \sqrt{r+s}\, R_K$, where R_K is the absolute value of the determinant of an arbitrary minor of rank $t = r+s-1$ of the matrix

$$\begin{pmatrix} \lambda(\varepsilon_1)_1 & & \lambda(\varepsilon_t)_1 \\ \vdots & \cdots & \vdots \\ \lambda(\varepsilon_1)_{t+1} & & \lambda(\varepsilon_t)_{t+1} \end{pmatrix}.$$

R_K is called the <u>regulator of K</u>.

<u>Proof</u>: In $(**)$ add all rows to one arbitrary row. Every entry will vanish

except for the entry in the first column which is $\sqrt{r+s} = \frac{r+s}{\sqrt{r+s}}$. $\square$

We saw the regulator appearing in Theorem 7.10 (Analytic class number formula):

Lecture 11

Theorem 7.10 (Analytic class number formula)

The residue of ζ_K at $z=1$ is given by

$$\lim_{z\to 1}(1-z)\zeta_K(z) = \frac{2^r (2\pi)^s h_K R_K}{\omega_K \sqrt{|d_K|}}$$

$$\lim_{z\to 1}(1-z)\zeta_K(z) = \operatorname{Res}_{z=1}\zeta_K(z)$$

where $\omega_K = \#$ roots of unity in K.
$= |\mu(K)|$.

§10 Extensions of Dedekind domains

From now we consider again the more general case:

$$\begin{array}{ccccccc} & & \mathrm{Frac}(A) & & \text{fin. extension} & & \\ \underline{\text{Ex}} & \mathbb{Q} & \subset & \overset{\shortparallel}{K} & \subset & L & \\ & \cup & & \cup & & \cup & \\ & \mathbb{Z} & \subset & \mathcal{O}_K = A & \subset & \mathcal{O} & \end{array}$$

Ex: K number field

A: Dedekind domain

$\mathcal{O}$: integral closure of A in L

Assume further that $\mathrm{char}(K) = 0$ or $|K| < \infty$.

Goal: Understand how prime ideals $\mathfrak{p} \subset A$ "behave" in $\mathcal{O}$.

Proposition 10.1

i) $\mathcal{O}$ is a Dedekind domain

ii) Every ideal of $\mathcal{O}$ is a finitely generated A-module.

Proof: • Since $\mathcal{O}$ is the integral closure of A it is integrally closed (Corollary 2.8)

• Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis of L/K with discriminent $d = d(\alpha_1, \dots, \alpha_n) \left(= \det(\sigma_i(\alpha_j))^2,\ \sigma_i : L \to \overline{K}\right)$

$\underset{\text{Prop 3.10}}{\neq} 0$

We can choose $\alpha_j \in \mathcal{O}$ and by Lemma 3.13

$$\mathcal{O} \subseteq A\frac{\alpha_1}{d} + \dots + A\frac{\alpha_n}{d} =: M.$$

M is a fin. gen. A-module and therefore by Prop. 1.40 noetherian.
Every ideal of $\mathcal{O}$ is contained in M and therefore fin. gen. A-module.
Therefore they are also fin. gen. $\mathcal{O}$-modules.
$\Longrightarrow$ $\mathcal{O}$ is noetherian.

• Let $\mathfrak{P} \neq 0$ be a prime ideal of $\mathcal{O}$.
Set $\mathfrak{p} = \mathfrak{P} \cap A$. This is a prime ideal in

the Dedekind domain A and therefore maximal.

$\Rightarrow A/\mathfrak{p}$ is a field.

The integral domain $\mathcal{O}/\mathfrak{p}$ is a fin. dim. $A/\mathfrak{p}$-vector space. The multiplication with an element $x \in \mathcal{O}/\mathfrak{p}$ $(\neq 0)$ is an injective endomorphism, i.e. surjective, and therefore every element in $\mathcal{O}/\mathfrak{p}$ has an inverse.

$\Rightarrow \mathcal{O}/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ is maximal. $\square$

Proposition 10.2 Let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$.

Proof: Since the factorization into prime ideals in A is unique, there exist a $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$.

Then $\pi A = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{p} \nmid \mathfrak{a}$, i.e $\mathfrak{p}+\mathfrak{a}=A$.

Therefore we can find $b \in \mathfrak{p}$ and $s \in \mathfrak{a}$ with $b+s=1$.

We have $s \notin \mathfrak{p}$, since otherwise $\mathfrak{p} = A$. Also

$$s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi A.$$

If we would have $\mathfrak{p}\mathcal{O} = \mathcal{O}$, we would get

$$s\mathcal{O} = s\mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O}.$$

But then $s = \pi x$ with $x \in \mathcal{O} \cap K = A$, since A is integrally closed. This would give $s \in (\pi) \subseteq \mathfrak{p}$ ↯. Therefore $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$. $\square$

Let $\mathfrak{p} \neq (0)$ be a prime ideal in A.
In $\mathcal{O}$ we have the unique factorization

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \qquad (\star)$$

whe $\mathfrak{P}_i$ are pairwise different prime ideals in $\mathcal{O}$ and $e_1, \dots, e_r \geq 1$.
The ideals $\mathfrak{P}_i$ are exactly those for which $\mathfrak{P}_i \cap A = \mathfrak{p}$.

We say $\mathfrak{P}_i$ lies over $\mathfrak{p}$ and write $\mathfrak{P}_i \mid \mathfrak{p}$.

Definition 10.3

i) The exponent e_i in (✱) is called the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$.

ii) The degree of the field extension

$$f_i = [\mathcal{O}/\mathfrak{P}_i : A/\mathfrak{p}]$$

is called the inertia degree of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Theorem 10.4 (Fundamental identity)

Let $\mathrm{char}(K)=0$ or $|K|<\infty$, $n=[L:K]$ and $\mathfrak{p} \subset A$ prime.

If $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ then

$$\sum_{i=1}^{r} e_i f_i = n.$$